DATENSCHUTZ UND BEWEIS BEI SMARTCARS

Johannes Scharf / Thomas Preiß

Rechtsanwaltsanwärter, CMS Reich-Rohrwig Hainz Rechtsanwälte GmbH
Gauermanngasse 2, 1010 Wien, AT
johannes.scharf@cms-rrh.com; https://cms.law/de/AUT/People/Johannes-Scharf

Wissenschaftlicher Dienst, Amt der Niederösterreichischen Landesregierung
Landausplatz 1, 3109 St. Pölten, AT
thomas.preiss@noel.gv.at

Schlagworte: ***Autonomes Fahren, Datenschutz, Personenbezug, Beweismittel, Beweisverwertungsverbot***

Abstract: *Autonomes Fahren ist mit schwierigen Rechtsfragen verbunden. Dieser Beitrag geht auf die datenschutzrechtliche Qualifikation von Sensordaten ein und zeigt, dass seit dem Urteil des EuGH zu Breyer eine differenzierte Betrachtungsweise erforderlich ist. Zudem wird erläutert, unter welchen Umständen rechtswidrig erlangte Aufzeichnungen im Verwaltungsverfahren als Beweismittel verwertet werden dürfen.*

1. Einleitung

Moderne Fahrzeuge sind schon jetzt mit zahlreichen Assistenzsystemen ausgestattet, die den Fahrer bei der Steuerung und Navigation entlasten sollen. Die technologische Entwicklung schreitet rasant voran und die allumfassende Vernetzung macht auch vor Fahrzeugen nicht halt. Die nächste Generation dieser «Smartcars» steht bereits in den Startlöchern und wird in absehbarer Zeit autonom («automatisiert») auf den Straßen unterwegs sein.[1] Verglichen mit heutigen Fahrzeugen sind diese mit weitaus besseren Sensoren ausgestattet, die ein noch deutlicheres Bild der Umgebung erfassen, und stärker mit der Umwelt und anderen Fahrzeugen vernetzt. Autonomes Fahren an sich bedeutet grundsätzlich nicht zwingend die Vernetzung des Fahrzeugs, da die Navigation auch ausschließlich im Fahrzeug mithilfe des Bordcomputers erfolgen könnte. Für eine exakte Navigation reichen jedoch die Sensoren (noch) nicht aus und die Fahrzeuge sind auf exakte Kartendaten angewiesen, die stets aktuell sein und daher über das Internet laufend aktualisiert werden müssen.[2] Ab 31. März 2018 müssen alle Neufahrzeuge auch mit dem automatischen Notrufsystem «eCall» ausgestattet sein, was einen Zugang zum Internet voraussetzt, da bei einem Unfall auch der Standort übermittelt wird. Ein autonomes Fahrzeug setzt damit letztendlich auch die Vernetzung mit dem Internet voraus. Aus diesem Grund ist die ganzheitliche Betrachtung von autonomen Fahrzeugen und einhergehender Vernetzung mit ihrer Umwelt erforderlich.

Das Auto wird mit anderen Fahrzeugen, Verkehrszeichen etc. vernetzt und damit Teil des «Internets der Dinge».[3] Das «Zusammenwachsen» von Internet und Auto stellt die ehemals «internetfreie» Zone des Automobils vor Herausforderungen, die ansonsten nur aus dem Cyberspace bekannt sind. Dazu gehören die Bedrohung durch Hacker und Viren sowie die mit Big Data und Cloud Computing verbundenen rechtlichen Herausforderungen.

Autonomes Fahren kann wesentlich zur Verbesserung der Sicherheit des Straßenverkehres beitragen, einen Beitrag zum Umweltschutz leisten und den Fahrkomfort erhöhen.[4] Moderne Fahrzeuge sammeln dabei eine Vielzahl von Daten. Die Vernetzung potenziert nicht nur die anfallenden Datenmengen, sondern auch die

---

1 Vgl. die AutomatFahrV, BGBl. II Nr. 402/2016, die Tests autonomer Fahrzeuge auf Straßen ermöglicht.

2 Weisser/Färber, Rechtliche Rahmenbedingungen bei Connected Car, MMR 2015, 506, S. 2.

3 Europäische Kommission, The Internet of Things. https://goo.gl/vDIx1G (alle Websites aufgerufen am 10. Januar 2017).

4 53. Deutscher Verkehrsgerichtstag 2015, Empfehlung Automatisiertes Fahren, S. 2.

rechtlichen Probleme. Die Datensammlung erzeugt zwingendermaßen Begehrlichkeiten von Gerichten, Verwaltungsbehörden, Versicherungen, Unfallgegnern, der Polizei etc.[5] Autonome Fahrzeuge sind daher mit technischen, rechtlichen,[6] ethischen und gesellschaftspolitischen Fragen verbunden.

Vor dem Hintergrund des jüngsten Urteils des EuGH zu *Breyer*,[7] das einem «ausufernden» Datenschutz eine Absage erteilt, geht dieser Beitrag auf die Frage ein, unter welchen Voraussetzungen Sensordaten als personenbezogene Daten zu qualifizieren sind. Weiters soll auf die, vermehrt im Zusammenhang mit sogenannten «Dashcams» auftretende, Frage eingegangen werden, ob möglicherweise rechtswidrig erlangte Beweismittel im verwaltungsbehördlichen Verfahren verwertet werden dürfen und ob der Zulassungsbesitzer bzw. Fahrer möglicherweise sogar verpflichtet ist, Aufzeichnungen seines Fahrzeugs herauszugeben.

2. Datenschutz

2.1. Schutzbereich des DSG

Das (österreichische) Datenschutzgesetz 2000 («**DSG**») ist, so wie die Datenschutz-RL 95/46/EG («**DSRL**»), nur auf «personenbezogene Daten» («**Daten**») anwendbar und versteht darunter (fast wortgleich mit der DSRL) «Angaben über Betroffene, deren Identität bestimmt oder bestimmbar ist».[8]

Die Identität des Betroffenen ist bestimmt, wenn Daten einer Person so zugeordnet sind, dass deren Identität direkt ersichtlich ist, z.B. in den meisten Fällen, wenn Name und Geburtsdatum vorliegen. Dabei ist es vom Kontext der jeweiligen Situation abhängig, welche Kombination von Daten für die Identifizierung ausreichend ist.[9]

Die «Bestimmbarkeit» als zweite Variante personenbezogener Daten bedeutet, dass die Identität einer Person erst mithilfe von Zusatzinformationen festgestellt werden kann. Zu denken ist hier beispielsweise an eine Personalnummer, die jederzeit mit dem Namen verknüpft werden kann. Nach den Vorgaben der DSRL ist eine Person dann als «bestimmbar» anzusehen, wenn sie direkt oder indirekt identifiziert werden kann, insbesondere durch Zuordnung zu einer Kennnummer oder zu einem oder mehreren spezifischen Elementen, die Ausdruck ihrer physischen, psychologischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität sind.

Vor allem in der deutschen Literatur herrscht eine rege Diskussion darüber, ob die Bestimmbarkeit objektiv, also absolut, oder relativ, aus Sicht des jeweiligen Verwenders der Daten, zu beurteilen ist.[10] Nach der DSRL und den Erläuterungen zum DSG sind alle Mittel zu berücksichtigen, die vernünftigerweise entweder von dem für die Verarbeitung Verantwortlichen (nach DSG «**Auftraggeber**») oder von einem Dritten eingesetzt werden könnten, um die betreffende Person zu bestimmen. Der Wortlaut (arg. «oder von einem Dritten») spricht grundsätzlich dafür, auf den datenschutzfreundlicheren, objektiven Ansatz der Bestimmbarkeit abzustellen. Dieser wird vor allem von den Datenschutzbehörden und ebenso von namhaften Autoren in der österreichischen Literatur vertreten.[11]

---

5 Vgl. die jüngsten Diskussionen, der Polizei Zugriff auf private Videos und Aufnahmen der Asfinag zu verschaffen: https://goo.gl/RbkE2N. Ebenso die Bestrebungen amerikanischer Behörden, Zugriff auf die Aufzeichnungen des Geräts «Alexa» von Amazon in einem Mordfall zu erhalten: http://nyti.ms/2iGPZ8I.

6 Die rechtliche Dimension umfasst insbesondere datenschutz-, haftungs- und verkehrsrechtliche Fragestellungen.

7 EuGH 19. Oktober 2016, C-582/14 (*Breyer*).

8 Beide Formen von Daten sind einander gleichgestellt und sind mit identischen Rechtsfolgen verbunden. Das DSG schützt zusätzlich zur DSRL Daten juristischer Personen und Personengemeinschaften. Auf die dem Unionsrecht fremde Kategorie der «indirekt personenbezogenen Daten» soll hier nicht eingegangen werden. Jahnel, EuGH: Dynamische IP-Adressen sind personenbezogene Daten, jusIT 2016/105 hält diese Kategorie für europarechtswidrig.

9 Jahnel, Handbuch Datenschutzrecht, Wien 2010, Rz. 3/75.

10 Jensen, BGH legt EuGH die Frage vor, ob IP-Adressen personenbezogene Daten sind, ZD-Aktuell 2014, 04460.

11 Jahnel, Handbuch Datenschutzrecht, Wien 2010, Rz. 3/77; Bergauer, Indirekt personenbezogene Daten, in: Jahnel (Hrsg.), Jahrbuch Datenschutzrecht 2011, Wien 2011, S. 55 vertritt offenbar den relativen Ansatz.

Diesbezüglich Aufschluss brachte das jüngste EuGH-Urteil zu *Breyer*: Der EuGH erteilte dem objektiven Ansatz und damit einem «ausufernden» Datenschutz eine Absage, da der Personenbezug aus Sicht des jeweiligen Verantwortlichen zu beurteilen sei. Dabei sei jedoch das Wissen solcher Dritter relevant, die vernünftigerweise vom Verantwortlichen zur Identifikation einer Person herangezogen werden könnten. Dies sei dann nicht der Fall, wenn die Identifizierung der betreffenden Personen gesetzlich verboten oder praktisch nicht durchführbar wäre, z.B. weil sie einen unverhältnismäßigen Aufwand an Zeit, Kosten und Arbeitskräften erfordern würde, sodass das Risiko einer Identifizierung *de facto* vernachlässigbar erschiene.[12] So gelangt der EuGH im Hinblick auf dynamische IP-Adressen zur Ansicht, dass diese für den Webseitenbetreiber personenbezogene Daten seien, wenn rechtliche Möglichkeiten bestünden, die es ihm erlauben, sich insbesondere im Fall von Cyberattacken an die zuständige Behörde zu wenden, um die fraglichen Informationen vom Internetzugangsanbieter zu erlangen und die Strafverfolgung einzuleiten.

Nach dem EuGH-Urteil ist es daher für die Qualifikation von Informationen als bestimmbare personenbezogene Daten der Umstand ausreichend, wenn der jeweilige Auftraggeber über Mittel verfügt, die er «vernünftigerweise» zur Identifikation einer Person einsetzen könnte.[13] Nicht gefordert ist jedoch, dass konkret im Einzelfall bereits eine Cyberattacke etc. stattgefunden hat, es reicht die «abstrakte» Möglichkeit, die Strafverfolgung einzuleiten.

2.2. Personenbezug

Die technische Aufrüstung des Fahrzeugs mit hochentwickelten Radarsensoren, Kameras und Laserscannern wird mit dem autonomen Fahren im Vergleich zu heutigen Fahrerassistenzsystemen wie Abstands- und Spurassistenten noch erheblich zunehmen. Neben steuerungsrelevanten Daten wie Lokation, Reiseziel, Geschwindigkeit können Sensoren auch die Fahrtauglichkeit des Fahrers erkennen. Dazu können dessen Augenbewegungen, Pulsfrequenz, Handfeuchtigkeit, Körperhaltung und Atemalkoholgehalt erfasst werden, wodurch Rückschlüsse auf dessen Gesundheit möglich sind.[14] Für die Kommunikation mit der IT des Fahrzeugherstellers wird üblicherweise eine «Vehicle Identification Number» (VIN) verwendet, wobei aus technischen Gründen dem Kommunikationspartner stets auch die dem Fahrzeug zugewiesene IP-Adresse bekannt ist. Der digitale Fingerabdruck der Fahrzeuginsassen vergrößert sich noch zusätzlich, wenn diese während des Fahrens digitale Angebote im Web nutzen und damit insbesondere Ziel von Tracking-Technologien werden.

Die Sensordaten des Fahrzeugs sowie vor allem die VIN lassen sich – ähnlich wie eine IP-Adresse oder ein Cookie[15] – zunächst nur einem bestimmten Fahrzeug eindeutig zuordnen. Personenbezogene Daten liegen aber dann vor, wenn sich die Daten einer bestimmten oder bestimmbaren Person zuordnen lassen. Die zum Personenbezug von Sensordaten vorhandene Literatur geht oftmals undifferenziert davon aus, dass es sich bei diesen bereits dann um personenbezogene Daten handle, wenn nur irgendein Dritter den Personenbezug herstellen könne.[16] Seit dem Urteil zu *Breyer* ist hinsichtlich Personenbezug jedoch eine differenzierte Sichtweise erforderlich.

Die VIN, die IP-Adresse sowie die Sensordaten können vom Hersteller aufgrund der vertraglichen Beziehung mit dem Fahrzeughalter diesem recht einfach namentlich zugeordnet werden. Für den Hersteller handelt es sich damit regelmäßig um personenbezogene Daten des Fahrzeughalters.

---

12 EuGH, Rs. *Breyer*, Rn. 46.

13 Die für einen Auftraggeber vernünftigerweise einsetzbaren Mittel können sich im Laufe der Zeit ändern und somit auch die Qualifikation von Informationen als personenbezogene Daten.

14 Lüdemann, Connected Cars ZD 2015, S. 247 (S. 248).

15 Jahnel, Handbuch Datenschutzrecht, Wien 2010, Rz. 3/82.

16 Kunnert, Das vernetzte Automobil aus datenschutzrechtlicher Sicht, ZVR 2015/242, S. 481 f. und offenbar Lüdemann, Connected Cars ZD 2015, S. 247 (S. 250) der von einer «objektiven» Bestimmbarkeit durch andere spricht; a.A. wohl Weisser/Färber, Rechtliche Rahmenbedingungen bei Connected Car, MMR 2015, 506, denen zufolge der Personenbezug aus Sicht des Navigationsgeräteherstellers etc. zu beurteilen sei («relativer Ansatz»).

Der Fahrzeughalter muss jedoch keineswegs auch immer der Fahrer im konkreten Fall sein. Vor allem bei Firmenfahrzeugen, aber auch bei Privatfahrzeugen muss nicht unbedingt der Fahrzeughalter selbst das Fahrzeug lenken. Auf dieses Problem der «falschen» Zuordnung eines Datums zu einer Person, das sich auch im Zusammenhang mit IP-Adressen bei wechselnden Nutzern eines Computers stellt, wird in der Literatur nur vereinzelt eingegangen. Der Personenbezug wird soweit ersichtlich bejaht.[17] In Anbetracht der Intention des europäischen Gesetzgebers, in der Gemeinschaft ein hohes Schutzniveau sicherzustellen, ist «im Zweifel» zunächst von personenbezogenen Daten auszugehen und der Personenbezug zu befürworten.[18]

Ebenso können Daten sonstiger Fahrzeuginsassen aufgezeichnet werden, wie Sitzposition, Gewicht, angelegter Sicherheitsgurt. Diese Daten stellen nur in Ausnahmefällen für den Hersteller personenbezogene Daten dar, wenn er diese mit identifizierenden Merkmalen, bspw. mit einer Benutzerkennung für vom Hersteller angebotene Multimediadienste, verknüpfen kann.

Abgesehen von den Fahrzeuginsassen werden auch andere Verkehrsteilnehmer und Passanten von den (visuellen) Sensoren autonomer Fahrzeuge erfasst. Das Spektrum reicht hier von bloßer Hinderniserkennung bis zur Aufzeichnung hochauflösender Bilder, aus denen Vorhersagen über das Verhalten von Fußgängern gewonnen werden können. Lüdemann postuliert Mustererkennung und maschinelles Lernen als unabdingbare Voraussetzungen, soll die Software in der Lage sein, das Fahrzeug mindestens genauso gut wie ein Mensch zu führen.[19] Dafür sind grundsätzlich Bilder mit hoher Auflösung erforderlich.

Bei Bild- und Videodaten handelt es sich nach herrschender Ansicht um bestimmbare personenbezogene Daten, wenn die technische Auflösung des Bildes eine Identifizierung zulässt.[20] Der Personenbezug von Bild- und Videodaten wurde vom EuGH in der Rs. *Ryneš* grundsätzlich bestätigt, sofern diese die Identifikation der betroffenen Person ermöglichen.[21] Im Lichtes der Rs. *Breyer* ist dieses Urteil wohl so zu verstehen, dass der EuGH bei einer Videoüberwachung durch Private offenbar davon ausgeht, dass diese über Mittel verfügen, die «vernünftigerweise» eingesetzt werden können, um die betreffende Person zu identifizieren.

Unsers Erachtens ist daher grundsätzlich anzunehmen, dass die Kameras von Smartcars personenbezogene Daten aufzeichnen, da die Aufnahmen vom Hersteller bspw. zur Klärung seiner Haftung bei einem Unfall mithilfe der Gerichte einer bestimmten Person zugeordnet werden können. Die Entscheidungen zu sogenannten «Dashcams» zeigen, dass auch für Private die Videoaufzeichnungen aus Fahrzeugen als personenbezogene Daten zu qualifizieren sind.

In diesem Zusammenhang tun sich schwierige Abgrenzungsfragen zur Videoüberwachung i.S.d. §§ 50a ff. DSG auf: Nach Ansicht der Datenschutzbehörde entscheidet der intendierte Zweck der Videoaufzeichnung, ob eine gewöhnliche Datenanwendung oder eine Videoüberwachung mit erhöhten Zulässigkeitsvoraussetzungen vorliegt. Sofern daher die visuellen Sensoren des Smartcars ausschließlich zur Navigation verwendet werden, liegt voraussichtlich keine Videoüberwachung, sondern eine sonstige Datenanwendung vor. Werden hingegen Daten (wenn auch nur kurzfristig) zwecks Verwendung als Beweismittel gespeichert, ist mit hoher Wahrschein-

---

17 Riesz, in: Riesz/Schilchegger (Hrsg.), TKG § 92 Rz. 13; Lechner, Datenschutz und Internet, in: Bauer/Reimer (Hrsg.), Handbuch Datenschutzrecht, Wien 2009, S. 214, 217; indirekt bejahend auch DSB 15. April 2016, DSB-D122.418/0002-DSB/2016 bei wechselnden Handynutzern; einschränkend insofern Jahnel, Handbuch Datenschutzrecht, Wien 2010, Rz. 3/76, der personenbezogene Daten unter Verweis auf die Rsp. der DSK nur bei «hohem Risiko der Identifizierung» annimmt; ebenso der EuGH, Rs. *Breyer*, Rn. 46, dem nach keine personenbezogenen Daten vorliegen, wenn «Risiko der Identifizierung» de facto vernachlässigbar erscheint; und Art-29-Datenschutzgruppe, Stellungnahme 4/2007, WP 136, S. 20 zu IP-Adressen bei anonymer Nutzung in Internetcafés.

18 Jahnel, Handbuch Datenschutzrecht, Wien 2010, Rz. 3/72; EuGH, 11. Dezember 2014, C-212/13 (*Ryneš*), Rn. 27 unter Verweis auf ErwGr. 10 DSRL.

19 Lüdemann, Connected Cars ZD 2015, S. 247 (S. 249).

20 Siehe dazu Jahnel, Handbuch Datenschutzrecht, Wien 2010, Rz. 3/77; VwGH 12. September 2016, Ro 2015/04/00117, Rn. 11; Nach Thiele, Die Trias von § 16 ABGB, § 78 UrhG und Datenschutz, in: Jahnel (Hrsg.), Jahrbuch Datenschutzrecht 2015, Wien 2015, S. 49 muss der Personenbezug mit «verhältnismäßigem Aufwand» herstellbar sein.

21 EuGH, Rs. *Ryneš*.

lichkeit von einer Videoüberwachung auszugehen.[22] Die höchstgerichtliche Rechtsprechung scheint solchen Dashcams nur einen äußerst schmalen Zulässigkeitsbereich zu gewähren.[23]

Weiters ist nicht abschließend geklärt, wann Bild- und Videoaufzeichnungen als sensible Daten einzustufen sind. Dies hätte zur Konsequenz, dass die Aufnahme ohne gesetzliche Grundlage nicht ohne Zustimmung der betroffenen Person erfolgen dürfte.[24] So kann gerade im Straßenverkehr nicht ausgeschlossen werden, dass die Kameras einen Unfall erfassen und Verletzte aufgezeichnet werden, womit Rückschlüsse auf die Gesundheit möglich wären und daher sensible Daten vorliegen könnten.

2.3. Fazit

Wie die Analyse zeigt, handelt es sich bei Sensordaten für den Hersteller regelmäßig um personenbezogene Daten.[25] Nach dem Breyer-Urteil ist der Personenbezug stets aus Sicht des jeweiligen Auftraggebers zu beurteilen und nicht wie bisher oftmals vertreten generell vom Personenbezug auszugehen. Dieselben Daten können daher für unterschiedliche Akteure eine andere rechtliche Qualität aufweisen.[26]

Daraus folgt, dass die Datenanwendung «Smartcar» vor Aufnahme der Verarbeitung im Datenverarbeitungsregister gemeldet werden muss (§ 17 DSG). Mit Bild- und Videoaufzeichnungen ist eine gewissen Rechtsunsicherheit verbunden, da nicht abschließend geklärt ist, ob es sich bei diesem um sensible Daten handelt. Das vom VwGH weitgehend bestätigte Urteil des BVwG zu Dashcams deutet jedenfalls in diese Richtung (Fn. 24). Die Qualifikation von Aufzeichnungen als sensible Daten hätte zur Folge, dass die Datenverarbeitung ohne spezielle gesetzliche Grundlage oder die Zustimmung sämtlicher Betroffener unzulässig wäre (§ 9 DSG). Überdies dürfte die Datenverarbeitung nicht ohne die vorherige Genehmigung der Datenschutzbehörde aufgenommen werden (§ 18 Abs. 2 DSG).

An den Gesetzgeber sei die Aufforderung gerichtet, eine geeignete datenschutzrechtliche Grundlage für Smartcars zu schaffen. Eine solche sollte auch verbindliche Standards für die Ausgestaltung (visueller) Sensoren festlegen. Die kommende Datenschutz-Grundverordnung 2016/679/EU («**DSGVO**») setzt die Prinzipien der DSRL fort und vermag diesbezüglich ebenso wenig für Klarstellung zu sorgen.

Aus Platzgründen kann auf die grundlegenden Voraussetzungen zur rechtmäßigen Datenverarbeitung[27] und weitere damit in Zusammenhang mit Smartcars auftretende Probleme nur hingewiesen werden.[28]

3. Der Beweis im Verwaltungsverfahren

§ 46 AVG ordnet im Verwaltungsverfahren eine grundsätzliche Unbeschränktheit der Beweismittel an, da die Erforschung der materiellen Wahrheit (§ 37 AVG) der Kern eines jeglichen behördlichen Verfahren ist. Das Agieren der Behörden hat auf Basis von Gesetzen (Art. 18 B-VG) als Unterstreichung dessen Legitimität zu erfolgen, sodass die Erlangung von Beweismitteln im Rahmen eines in diesem Sinne rechtmäßigen Handelns zu geschehen hat. Da als Rechtmäßigkeit Unbeschränktheit angeordnet wird, stellen Beweisverbote[29] einen

---

22 Schmidl, Die Videoüberwachung i.S.d. DSG 2000, jusIT 2015/26.

23 Thiele/Jahnel, VwGH: «Dashcam» grundsätzlich zulässig, jusIT 2016/106; bisher wurde die Registrierung sämtlicher «Dashcams» von der Datenschutzbehörde abgelehnt.

24 Ablehnend Knyrim, Dako 2015/4 mit Verweis auf EuGH, Rs. *Ryneš*; Knyrim, Bilddaten: immer sensibel?, jusIT 2016/102; a.A. Bergauer, Die Einordnung von Bilddaten erkennbarer Personen im Datenschutzrecht, jusIT 2016/103 mit Verweis auf BVwG 30. Januar 2015, W214 2011104-1 zu Dashcam.

25 Es sind Konstellationen denkbar, in denen auch der (private) Fahrer als datenschutzrechtlicher Auftraggeber anzusehen ist. Die damit verbundenen datenschutzrechtlichen Fragen bleiben einer weiteren Abhandlung vorbehalten.

26 Auf weitere Fragen des Personenbezugs bei häufig wechselnden Benutzern (bspw. bei Mietfahrzeugen) oder im Zusammenhang mit Bewegungsprofilen kann hier aus Platzgründen nur hingewiesen werden.

27 Knyrim, Datenschutzrecht[3], Manz, Wien 2015, S. 121 f.

28 Siehe u.a. Kunnert, Das vernetzte Automobil aus datenschutzrechtlicher Sicht, ZVR 2015/242 und die in diesem Artikel referenzierte Literatur.

29 Vgl. Frieberger, Beweisverbote im Verwaltungsverfahren, Verlag Österreich, Wien 1997, S. 31.

Ausnahmetatbestand dar. Der österreichische Gesetzgeber ordnet diese selten an, sodass derartige Verbote aus dem dogmatischen Zusammenhang zu erschließen sind.

Jahnel hat dies im Zusammenhang mit der Verwendung von Daten als Beweismittel untersucht und postuliert, dass die Frage des Bestehens oder Nichtbestehens von Beweisverwertungsverboten auf Grundlage der entsprechenden verfahrensrechtlichen Bestimmungen bzw. der dazu ergangenen Judikatur zu prüfen ist.[30] So kann aus der Anordnung der Unbeschränktheit der Beweismittel etwa gefolgert werden, dass zur Rechtmäßigkeit der Datenverarbeitung beim Empfänger keine geschlossene Kette rechtmäßiger Datenverwendung bei allen zuvor verantwortlichen Auftraggebern vorliegen muss.[31] Verwendet eine Behörde «zweifelhafte» Daten zum Beweis einer (verwaltungs)strafrechtlich relevanten Tat, für deren Verfolgung sie unstrittig zuständig ist, dann liegt die geforderte Rechtmäßigkeit vor.

Dogmatische Überlegungen und die Entwicklung in der Judikatur des VwGH führen für das Verwaltungsverfahren zu dem Grundsatz, dass die Berücksichtigung von Beweisergebnissen, welche auf gesetzwidrige Weise gewonnen wurden, zur Ermittlung der materiellen Wahrheit dann unzulässig ist, wenn das Gesetz dies anordnet oder wenn die Verwertung des betreffenden Beweisergebnisses dem Zweck des durch seine Gewinnung verletzten Verbotes widerspräche.[32]

Unzweifelhaft steht einer gänzlich unbeschränkten Beweisfindung das Nemo-tenetur-Prinzip entgegen, das besagt, sich nicht selbst beschuldigen zu müssen (Art. 90 B-VG, Art. 6 EMRK). So der Gesetzgeber keine Herausgabepflicht normiert, besteht seitens der Person, in deren Sphäre das Beweismittel fällt, das Recht, in diesem Sinne zu handeln. Adäquate, dem öffentlichen Interesse dienende Einschränkungen vorbehaltlos gewährter Grundrechte[33] im Rahmen einer allgemeinen Auskunftspflicht können vorgesehen werden.

4. Wem gehören die Daten?

Obschon Daten dem Wesen nach als «unkörperliche Sache» im Sinne des Zivilrechts betrachtet werden könnten, ist die herrschende Meinung, dass an Daten kein sachenrechtliches Eigentum begründet werden kann.[34] Dem Grunde nach lässt sich aber anhand der Datenschutzprinzipien (sei es nach dem DSG oder der DSGVO) diese Frage «elegant umschiffen», da ja die «beliebige Verwendung von Sachen» durch den Eigentümer nach §§ 353 ff. ABGB nicht vorliegt. Bei Daten kommt es nicht auf die «Sphäre der Entstehung»[35] sondern auf den «Dateninhalt» an, um auf die tatsächlich vorliegende «beliebige Verwendbarkeit» (§ 6 DSG, Art. 5 DSGVO) Schließen zu können. Es kommt daher auf die Zulässigkeit und Rechtmäßigkeit einer Datenanwendung und weniger auf eine allfällig mögliche sachenrechtliche Zuordnung an. Dies wird weiter durch die im Folgenden vorgestellten Begriffe der «externen» und «internen» Daten der im Verkehrssystem Straße verfangenen «Subsysteme» klar.

Neben den im Datenschutzrecht vorgesehenen Prüfschritten zeigt Rannenberg[36] Möglichkeiten und Risiken auf, die darin bestehen, allfällig technisch nützliche Datenanwendungen in diesem Bereich vorzusehen. Das im europäischen Kontext vorgesehene hohe Datenschutzniveau ist auch in diesen Bereichen aufrecht zu erhalten, sodass eventuell sinnvolle Überwachungsmöglichkeiten nur innerhalb eines unbedenklichen Rechtsrahmens vorgesehen werden können. Rannenberg schlägt vor zu prüfen,

---

30 Jahnel, Handbuch Datenschutzrecht, Wien 2010, S. 221.

31 Jahnel, Handbuch Datenschutzrecht, Wien 2010, S. 222.

32 Vgl. etwa VwGH 15. Mai 2008, 2007/09/0306, weiters auch Frieberger, Beweisverbote im Verwaltungsverfahren, Verlag Österreich, Wien 1997, S. 233, zusammenfassend, der Gleiches aus Art. 6 EMRK folgert («fair trial»).

33 Vgl. Frieberger, Beweisverbote im Verwaltungsverfahren, Verlag Österreich, Wien 1997, S. 73.

34 Staudegger, Zur Zulässigkeit des Handels mit Daten aus Anlass der Weitergabe von «Gesundheitsdaten», ÖJZ 2014/21, S. 110.

35 Wohl sachenrechtlich nicht korrekt wollen wir doch den Begriff des «Dateneigentümers» verwenden.

36 Vgl. Preiss, Die Bedeutung der Risikoanalyse für den Rechtsschutz bei automatisierten Verwaltungsstrafverfahren, Dissertation, Universität Wien 2015, S. 153.

1. ob diese als «gelindestes Mittel» erforderlich ist, den geforderten Zweck zu erfüllen,
2. ob der Betroffene ausreichend informiert ist und
3. ob eine allfällige Weitergabe der Daten durch ihn selbst entschieden werden kann.

Die weitere Technisierung des «Verkehrssystem Straße»[37], das sowohl behördliches Handeln als auch die Art der Teilnahme an diesem System umfasst, wird nicht mit den bisherigen Normen das Auslangen finden und ist vom Gesetzgeber grundrechtskonform anzupassen. Empfehlungen des Deutschen Verkehrsgerichtstags[38] sehen bei der Gestaltung von Datenanwendungen die Unabdingbarkeit von Transparenz und Wahlfreiheit, der verständlichen Information bei Vertragsabschluss, die Unterbindbarkeit von freiwilligen Datenübermittlungen, der Sicherstellung eines ausreichenden Schutzniveaus bei gesetzlich vorgeschriebenen Datenübermittlungen sowie deren grundrechtskonforme Anwendungen bei behördlichen Verfahren als erforderlich an.

5. Zweck behördlicher Verfahren

Wie eingangs dargestellt, hat ein behördliches Verfahren (vgl. hiezu die Ausführungen zu § 46 AVG) die materielle Wahrheit über einen Sachverhalt herauszufinden und diese als Grundlage einer verwaltungsrechtlichen Entscheidung heranzuziehen. Die Rechtmäßigkeit der Verwendung der Daten eines autonomen Systems sei unterstellt, sodass zu prüfen ist, inwieweit diese Verwendung durch die Behörde vom «Dateneigentümer» beeinflusst werden kann.

5.1. Waffengleichheit

Mithilfe obiger Überlegungen und der Analyse der einschlägigen Judikatur[39] kann festgestellt werden, dass die gelebte Praxis darin besteht, Ergebnisse von automatisierten Überwachungen im Falle des Vorliegens einer gültigen Eichung als «richtig» zu betrachten. Nur im Falle einer leicht feststellbaren Unrichtigkeit besteht seitens der Judikatur Anlass, das Ergebnis der elektronischen Messung bzw. Überwachung berechtigt anzuzweifeln. Dem im Verwaltungsstrafverfahren Beschuldigten oder der Partei im Verwaltungsverfahren wird im Normalfall ein Gegenbeweis nicht gelingen, da einerseits keine wirksamen Beweismittel vorliegen werden und andererseits ein allgemeiner Hinweis auf vermutete Fehlerhaftigkeit nicht als ausreichende Argumentation seitens der Behörde angesehen werden wird.

6. Daten zur Zweckerreichung in grundrechtverträglicher Art

Es ist unstrittig, dass eine Steuerung autonomer Fahrzeuge einer Vielzahl von Daten bedarf. Es soll nun festgestellt werden, inwieweit diese im oben genannten Sinne der «Waffengleichheit» seitens der Behörde oder der Partei legitim – also keinem Beweisverwertungsverbot entgegenstehend – verwendet werden können. Diese können in zwei Gruppen – gleichsam in der Form eines Katalogs – in Abhängigkeit der grundsätzlichen Quelle der Daten geteilt werden. Wir verwenden die Begriffe der «internen» und der «externen» Daten. Diese Daten sind zum Teil geeignet, in einen Personenbezug gesetzt zu werden, wobei hier die jüngste, klarstellende Judikatur des EuGH[40] und des VwGH[41] zu beachten ist.

Die Begriffe selbst leiten sich aus dem betrachteten System des «autonomfahrenden Fahrzeugs und dessen Agieren im Verkehrssystem Straße» und dessen Grenzen ab. Daten, die innerhalb des Fahrzeugs (Motorsteue-

---

37 Vgl. Rossnagel, Grundrechtsausgleich beim vernetzten Automobil – Herausforderungen, Leistungsfähigkeit und Gestaltungsbedarf des Rechts, in: Datenschutz und Datensicherheit – DuD 6/2015, S. 353 ff. (S. 353–354), zitiert in: Preiss, Die Bedeutung der Risikoanalyse für den Rechtsschutz bei automatisierten Verwaltungsstrafverfahren, Dissertation, Universität Wien 2015, S. 157, Fn. 519.

38 Vgl. 52. Deutscher Verkehrsgerichtstag 2014. https://goo.gl/3bzVWp.

39 Vgl. Preiss, Die Bedeutung der Risikoanalyse für den Rechtsschutz bei automatisierten Verwaltungsstrafverfahren, Dissertation, Universität Wien 2015, S. 10f, 148.

40 Vgl. EuGH, Rs. *Breyer*, sowie Jahnel, EuGH: Dynamische IP-Adressen sind personenbezogene Daten, jusIT 2016/105.

41 Vgl. Thiele/Jahnel, VwGH: «Dashcam» grundsätzlich zulässig, jusIT 2016/106.

rung, physikalische Daten als Ergebnis der Fahrdynamik, Interaktion mit geographischen Positionierungssystemen etc.) oder durch Bezugnahme auf absolut wirkende Referenzgrößen entstehen, seien in diesem Sinne als intern charakterisiert. Zur Unterstreichung dieser Eigenschaft fordern wir, dass keinerlei Personenbezug mit Ausnahme zu allfälligen Fahrzeuginsassen gegeben ist.

Externe Daten entstehen durch die «Kommunikation» des autonomen Fahrzeugs mit Systemen, die zu den die internen Daten liefernden Systemen verschieden sind. Dies werden regelmäßig Ergebnisse von Umgebungsscans durch bildgebende Verfahren sowie Daten, die aus der Abfrage genormter elektronischer Schnittstellen gewonnen werden, sein. Diese sind in deren Anlage grundsätzlich mit Datenverarbeitungen von Dashcams vergleichbar, sodass anhand der hiezu bereits erfolgten Judikatur erschlossen werden kann, wie das Datenschutzthema zu bewerten ist. Wir unterstellen, dass die gewonnenen Daten bereits nach dem Grundsatz «Privacy by Design»[42] gewonnen werden. Für ein richtiges Reagieren im Verkehrssystem Straße ist ein Personenbezug nicht erforderlich – es wird ausreichen, dass erkannt wird, dass nun Interaktion im engen und weiten Sinn mit einer natürlichen Person[43] erfolgt. So ergibt sich folgende generische Tabelle, gleichsam als Katalog, wobei neben Kategorie, der Personenbezug, die Erfordernis einer datenschutzfreundlichen Implementierung und einer allfälligen Gleichwertigkeit zu automatischen Überwachungssystemen angegeben ist:

Art	**Privacy by Design**	**Personenbezug**[44]	**Beachtliche Daten (vgl. 5.1.)**
interne Daten	ja	nein; evtl. nach Einwilligung	wenn im «Smartcar» vorgesehen
externe Daten	ja	nein (vgl. Fn. 43)	wenn im «Smartcar» vorgesehen

7. Fazit

Daten können, so es zu deren «Erstellung» keinen gesetzlichen Auftrag gibt (z.B. «Fahrtenschreiber») nach dem Nemo-tenetur-Prinzip nur dann im Verwaltungsverfahren als Beweismittel herangezogen werden, wenn der «Beschuldigte» zustimmt (Beweisverwertungsverbot aufgrund der «Selbstbelastung»). Hiezu ist es nicht wesentlich, ob es sich um interne oder externe Daten mit oder ohne Personenbezug handelt, da das «nicht verhandelbare» Selbstbelastungsverbot vorgeht.

Im Sinne der «Waffengleichheit» im Verwaltungsverfahren sind vor allem interne Daten seitens der Behörden als gleichwertig zu von Aufsichtsorganen oder automatischer Überwachung entstandenen Daten zu sehen. Dies ist damit zu begründen, dass die Genehmigung autonomer Fahrzeuge auf eine sichere Sensorik nach dem Stand der Technik achten wird müssen.

So im Sinne der Entscheidung «Breyer» externe Daten keinen Personenbezug aufweisen, sind diese ebenfalls in diesem Sinne zu berücksichtigen. Insgesamt ist aber – wie bereits oben angemerkt – seitens des Gesetzgebers sicherzustellen, dass das im Verfassungsrang stehende Nemo-tenetur-Prinzip allen Vereinfachungsbestrebungen im Verwaltungsverfahren vorgeht.

---

42 Vgl. DSGVO, ErwGr. 78.

43 Vgl. hiezu den Lösungsvorschlag zu «Google Street View» durch Knoll, Zur datenschutzrechtlichen (Un)Zulässigkeit von Google Street View, jusIT 2010/10, sowie Rannenberg, Nutzbarmachung zusätzlicher Daten – Möglichkeiten und Risiken, in: Mauerer et al. (Hrsg.), Autonomes Fahren, Berlin 2015, S. 515 (S. 531). So die technischen Voraussetzungen vorliegen, kann ausreichender Datenschutz sichergestellt werden, wenn nach Herbeiführen der richtigen Aktion des Smartcars keine Speicherung von personenbezogenen Daten in erkennbarer Form erfolgt.

44 Wir gehen bei dieser Angabe davon aus, dass die Systeme «datenschutzfreundlich» implementiert wurden. Andernfalls ist durch Sicherstellung der Einwilligung des «Dateneigentümers», die Rechtmäßigkeit des Personenbezugs herzustellen.